

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

## In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*5834 NE 75th Street, apt B208, Seattle, WA 98115 and  
Android phone, model 1+, phone number 206-316-6268

Case No.

MJ18-568

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-1 and A-2, which is incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-1 and B-2, which is incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

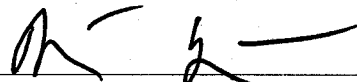
The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21, U.S.C. §§ 841(a)(1), 846	Distribution of Controlled Substances, Possession of Controlled Substances with Intent to Distribute, and Conspiracy to do the same.

The application is based on these facts:

Please see Affidavit of U.S. Postal Inspector Michael Fischlin

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's signature

 Michael Fischlin, U.S. Postal Inspector  
 Printed name and title

Sworn to before me and signed in my presence.

Date:

Dec 11, 2018

City and state: Seattle, Washington
  
 Judge's signature

 James P. Donohue, United States Magistrate Judge  
 Printed name and title

**AFFIDAVIT OF MICHAEL FISCHLIN**

STATE OF WASHINGTON )  
 )  
COUNTY OF KING ) SS

I, Michael Fischlin, an Inspector with United States Postal Inspection Service (“USPIS”), Seattle, Washington, having been duly sworn, state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Postal Inspector with the USPIS and have been so employed since June 2016. I am currently assigned to the Seattle Division, Prohibited Mail Narcotics Team, where I investigate controlled substances transported via the United States Mail. I have attended a one-week training course presented by the USPIS addressing narcotics investigations and trends in narcotics mailings. At that training, subject matter experts taught current trafficking trends and suspicious parcel recognition.

2. Prior to becoming a Postal Inspector, I was employed as a Special Agent (“SA”) of the United States Secret Service (“USSS”). As part of my training, I completed the Federal Law Enforcement Training Center (“FLETC”) Criminal Investigator Training Program as well as the USSS SA Training Program. While employed by the USSS, I was trained in computer forensics. Prior to joining the USSS, I served four years of active duty in the United States Marine Corps as a military policeman.

3. As a Postal Inspector, I am authorized to investigate crimes involving federal offenses relating to the United States Postal Service (“USPS”). During the course of my law enforcement career, I have conducted or participated in criminal investigations involving access device fraud, bank fraud, computer fraud, counterfeit currency and securities, identity theft, illegal narcotics, mail theft, robbery, and wire fraud. My duties have included planning the execution of search warrants; securing and searching premises; seizing documents, records and other evidence; and interviewing witnesses.

4. As discussed below, MATTHEW WITTERS sold drugs on dark web marketplaces under the handles “kakashisan” and “sayNOtoCUSTOMS,” which were shipped via the USPS. WITTERS completed approximately 2,938 orders on the dark web under the listed monikers for approximately 1,271 bitcoins, valued at approximately \$764,588 at the time of sales.

# **PURPOSE OF AFFIDAVIT**

5. This affidavit is submitted in support of an application for search warrants for the following property:

a. The residence located at 5834 NE 75th Street, apt B208, Seattle, WA 98115, to include the computer described in paragraph 17, all further described in Attachment A-1, which is incorporated herein by reference (hereafter the “SUBJECT RESIDENCE”).

b. The cellular phone belonging to MATTHEW WITTERS, *i.e.*, Android phone, model 1+, phone number 206-316-6268, as further described in Attachment A-2 (hereafter the “SUBJECT PHONE”).

6. As set forth below, I submit that the property described above contains evidence of drug trafficking, in violation of Title 21, United States Code, Section 841(a)(1), including conspiracy to distribute controlled substances, in violation of Title 21, United States Code, Section 846. I seek authority to seize the items described in Attachments B, which are incorporated herein by reference.

# **SUMMARY OF PROBABLE CAUSE**

13. On December 10, 2018, I obtained a search and seizure warrant in this matter. A copy of my affidavit is attached as Exhibit C, and is incorporated by reference.<sup>1</sup>

<sup>1</sup> Agents executed these warrants on December 10 and 11, 2018, seizing a substantial amount of assets. WITTERS was arrested by complaint on December 10 and is currently detained at the Federal Detention Center.

1       14. On December 10, 2018, MATTHEW WITTERS's girlfriend, who lives  
2 with WITTERS at the SUBJECT RESIDENCE, contacted the Seattle Police Department.  
3 She said she was worried that WITTERS had not returned to the residence. She said she  
4 feared that he had suffered harm, noting that WITTERS was selling fentanyl to a  
5 particular individual named Vince. She thus appeared unaware that WITTERS had been  
6 arrested.

7       15. On December 11, 2018, HSI contacted WITTERS's girlfriend. She said  
8 that she had looked at the SUBJECT PHONE the day before and saw an old message  
9 relating to the sale of fentanyl from WITTERS to a person named "Vince." She said that  
10 she contacted WITTERS's family, and that his mother had retrieved the SUBJECT  
11 PHONE. She advised that the phone was an Android phone, model 1+, phone number  
12 206-316-6268. According to a records check, WITTERS's mother lives in Burien.

13       16. She said that Vince owed WITTERS between \$1800 to \$3000 as a drug  
14 debt. She said that there was fentanyl in the SUBJECT RESIDENCE, which she then  
15 showed agents.

16       17. She said that neither she nor WITTERS was employed and that they were  
17 both opiate users. An HSI agent noticed that there was a computer that was open in the  
18 living room. The computer was a Tower, ASUS model, v12xT. The computer appeared  
19 to show a cryptocurrency trading page. WITTERS's girlfriend said that WITTERS  
20 invested in and traded Bitcoin. I believe that this computer contains evidence of drug  
21 trafficking. As detailed in the prior affidavit, there is probable cause to believe that  
22 WITTERS obtained the significant bulk of his wealth, including Bitcoins and other  
23 cryptocurrency, from drug trafficking. There is probable cause to believe that the  
24 computer will have evidence of the Bitcoins and cryptocurrency that WITTERS acquired,  
25 including the amount, timing, and source.

**TRAINING AND EXPERIENCE REGARDING CELLULAR PHONES**

18. Based upon my training and experience, and conversations with other experienced law enforcement agents and officers who have been involved in narcotics cases, I know the following:

19. Drug dealers regularly use cell phones, Blackberries, and other electronic communication devices to further their illegal activities. As a result, evidence of drug dealing can often be found in text messages, address books, call logs, photographs, emails, text messaging or picture messaging applications, videos, and other data that is stored on cell phones, Blackberries, and other electronic communication devices. Additionally, the storage capacity of such devices allows them to be used for the electronic maintenance of ledgers, pay/owe logs, drug weights and amounts, customers contact information, not only during the period of their drug trafficking violations but also for a period of time extending beyond the time during which the trafficker actually possesses/controls illegal controlled substances. The records are kept in order to maintain contact with criminal associates for future transactions and so that the trafficker can have records of prior transactions for which the trafficker might still be owed money or might owe someone else money.

**SEARCH AND SEIZURE OF DIGITAL MEDIA**

20. As described above and in Attachment B-1, this application seeks permission to search for the items listed in Attachment B-1 that might be found on the SUBJECT RESIDENCE, including the computer that is described in paragraph 17.

21. In order to examine the digital media seized in a forensically sound manner, law enforcement personnel, with appropriate expertise, will conduct a forensic review of any digital media seized. The purpose of using specially trained computer forensic examiners to conduct the imaging of any digital media, or digital devices is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always

1 necessary to separate these duties. Computer forensic examiners often work closely with  
2 investigative personnel to assist investigators in their search for digital evidence.  
3 Computer forensic examiners are needed because they generally have technological  
4 expertise that investigative agents do not possess. Computer forensic examiners,  
5 however, may lack the factual and investigative expertise that an investigative agent may  
6 possess. Therefore, computer forensic examiners often work closely together. It is  
7 intended that warrant will provide authority for the affiant to forensically review, or seek  
8 the assistance of others in HSI or within other law enforcement agencies to assist in the  
9 forensic review of any digital

10 22. I also know the following:

11 a. Based on my knowledge, training, and experience, your affiant  
12 knows that computer files or remnants of such files can be recovered months or even  
13 years after they have been downloaded onto a storage medium, deleted, or viewed via the  
14 Internet. Electronic files downloaded to a storage medium can be stored for years at little  
15 or no cost. Even when files have been deleted, they can be recovered months or years  
16 later using forensic tools. This is so because when a person “deletes” a file on a  
17 computer, the data contained in the file does not actually disappear; rather, that data  
18 remains on the storage medium until it is overwritten by new data.

19 b. Therefore, deleted files, or remnants of deleted files, may reside in  
20 free space or slack space—that is, in space on the storage medium that is not currently  
21 being used by an active file—for long periods of time before they are overwritten. In  
22 addition, a computer’s operating system may also keep a record of deleted data in a  
23 “swap” or “recovery” file.

24 c. Wholly apart from user-generated files, computer storage media—in  
25 particular, computers’ internal hard drives—contain electronic evidence of how a  
26 computer has been used, what it has been used for, and who has used it. To give a few  
27 examples, this forensic evidence can take the form of operating system configurations,  
28 artifacts from operating system or application operation, file system data structures, and



1 virtual memory “swap” or paging files. Computer users typically do not erase or delete  
2 this evidence, because special software is typically required for that task. However, it is  
3 technically possible to delete this information.

4 d. Similarly, files that have been viewed via the Internet are sometimes  
5 automatically downloaded into a temporary Internet directory or “cache.”

6 e. Digital storage devices may also be large in capacity, but small in  
7 physical size. Because those who are in possession of such devices also tend to keep them  
8 on their persons, especially when they may contain evidence of a crime. Digital storage  
9 devices may be smaller than a postage stamp in size, and thus they may easily be hidden  
10 in a person’s pocket.

11 23. As further described in Attachment B-1, this application seeks permission  
12 to locate not only computer files that might serve as direct evidence of the crimes  
13 described on the warrant, but also for forensic electronic evidence that establishes how  
14 computers were used, the purpose of their use, who used them, and when. There is  
15 probable cause to believe that this forensic electronic evidence will be on the device  
16 described in Attachment B-1 because:

17 a. Data on the digital storage medium or digital devices can provide  
18 evidence of a file that was once on the digital storage medium or digital devices but has  
19 since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has  
20 been deleted from a word processing file). Virtual memory paging systems can leave  
21 traces of information on the storage medium that show what tasks and processes were  
22 recently active. Web browsers, email programs, and chat programs store configuration  
23 information on the storage medium that can reveal information such as online nicknames  
24 and passwords. Operating systems can record additional information, such as the  
25 attachment of peripherals, the attachment of USB flash storage devices or other external  
26 storage media, and the times the computer was in use. Computer file systems can record  
27 information about the dates files were created and the sequence in which they were  
28 created, although this information can later be falsified.

1           b. As explained herein, information stored within a computer and other  
2 electronic storage media may provide crucial evidence of the “who, what, why, when,  
3 where, and how” of the criminal conduct under investigation, thus enabling the United  
4 States to establish and prove each element or alternatively, to exclude the innocent from  
5 further suspicion. In my training and experience, information stored within a computer  
6 or storage media (e.g., registry information, communications, images and movies,  
7 transactional information, records of session times and durations, internet history, and  
8 anti-virus, spyware, and malware detection programs) can indicate who has used or  
9 controlled the computer or storage media. This “user attribution” evidence is analogous  
10 to the search for “indicia of occupancy” while executing a search warrant at a residence.  
11 The existence or absence of anti-virus, spyware, and malware detection programs may  
12 indicate whether the computer was remotely accessed, thus inculcating or exculpating the  
13 computer owner. Further, computer and storage media activity can indicate how and  
14 when the computer or storage media was accessed or used. For example, as described  
15 herein, computers typically contain information that log: computer user account session  
16 times and durations, computer activity associated with user accounts, electronic storage  
17 media that connected with the computer, and the IP addresses through which the  
18 computer accessed networks and the internet. Such information allows investigators to  
19 understand the chronological context of computer or electronic storage media access, use,  
20 and events relating to the crime under investigation. Additionally, some information  
21 stored within a computer or electronic storage media may provide crucial evidence  
22 relating to the physical location of other evidence and the suspect. For example, images  
23 stored on a computer may both show a particular location and have geolocation  
24 information incorporated into its file data. Such file data typically also contains  
25 information indicating when the file or image was created. The existence of such image  
26 files, along with external device connection logs, may also indicate the presence of  
27 additional electronic storage media (e.g., a digital camera or cellular phone with an  
28 incorporated camera). The geographic and timeline information described herein may



1 either inculcate or exculpate the computer user. Last, information stored within a  
2 computer may provide relevant insight into the computer user's state of mind as it relates  
3 to the offense under investigation. For example, information within the computer may  
4 indicate the owner's motive and intent to commit a crime (e.g., internet searches  
5 indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program  
6 to destroy evidence on the computer or password protecting/encrypting such evidence in  
7 an effort to conceal it from law enforcement).

8 c. A person with appropriate familiarity with how a computer works  
9 can, after examining this forensic evidence in its proper context, draw conclusions about  
10 how computers were used, the purpose of their use, who used them, and when.

11 d. The process of identifying the exact files, blocks, registry entries,  
12 logs, or other forms of forensic evidence on a storage medium that are necessary to draw  
13 an accurate conclusion is a dynamic process. While it is possible to specify in advance  
14 the records to be sought, computer evidence is not always data that can be merely  
15 reviewed by a review team and passed along to investigators. Whether data stored on a  
16 computer is evidence may depend on other information stored on the computer and the  
17 application of knowledge about how a computer behaves. Therefore, contextual  
18 information necessary to understand other evidence also falls within the scope of the  
19 warrant.

20 e. Further, in finding evidence of how a computer was used, the  
21 purpose of its use, who used it, and when, sometimes it is necessary to establish that a  
22 particular thing is not present on a storage medium. For example, the presence or  
23 absence of counter-forensic programs or anti-virus programs (and associated data) may  
24 be relevant to establishing the user's intent.

25 24. In most cases, a thorough search of a premises for information that might  
26 be stored on digital storage media or other digital devices often requires the seizure of the  
27 digital devices and digital storage media for later off-site review consistent with the  
28 warrant. In lieu of removing storage media from the premises, it is sometimes possible to

1 make an image copy of storage media. Generally speaking, imaging is the taking of a  
2 complete electronic picture of the digital media's data, including all hidden sectors and  
3 deleted files. Either seizure or imaging is often necessary to ensure the accuracy and  
4 completeness of data recorded on the storage media, and to prevent the loss of the data  
5 either from accidental or intentional destruction. This is true because of the following:

6 a. *The time required for an examination.* As noted above, not all  
7 evidence takes the form of documents and files that can be easily viewed on site.  
8 Analyzing evidence of how a computer has been used, what it has been used for, and who  
9 has used it requires considerable time, and taking that much time on premises could be  
10 unreasonable. As explained above, because the warrant calls for forensic electronic  
11 evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage  
12 media to obtain evidence. Storage media can store a large volume of information.  
13 Reviewing that information for things described in the warrant can take weeks or months,  
14 depending on the volume of data stored, and would be impractical and invasive to  
15 attempt on-site.

16 b. *Technical requirements.* Computers can be configured in several  
17 different ways, featuring a variety of different operating systems, application software,  
18 and configurations. Therefore, searching them sometimes requires tools or knowledge  
19 that might not be present on the search site. The vast array of computer hardware and  
20 software available makes it difficult to know before a search what tools or knowledge  
21 will be required to analyze the system and its data on the Premises. However, taking the  
22 storage media off-site and reviewing it in a controlled environment will allow its  
23 examination with the proper tools and knowledge.

24 c. *Variety of forms of electronic media.* Records sought under this  
25 warrant could be stored in a variety of storage media formats that may require off-site  
26 reviewing with specialized forensic tools.

27 25. Searching computer systems is a highly technical process that requires  
28 specific expertise and specialized equipment. There are so many types of computer

1 hardware and software in use today that it is rarely possible to bring to the search site all  
2 the necessary technical manuals and specialized equipment necessary to consult with  
3 computer personnel who have specific expertise in the type of computer, operating  
4 system, or software application being searched.

5 26. The analysis of computer systems and storage media often relies on  
6 rigorous procedures designed to maintain the integrity of the evidence and to recover  
7 "hidden," mislabeled, deceptively named, erased, compressed, encrypted or password-  
8 protected data, while reducing the likelihood of inadvertent or intentional loss or  
9 modification of data. A controlled environment such as a laboratory, is typically required  
10 to conduct such an analysis properly.

11 27. The volume of data stored on many computer systems and storage devices  
12 will typically be so large that it will be highly impractical to search for data during the  
13 execution of the physical search of the premises. The hard drives commonly included in  
14 desktop computers are capable of storing millions of pages of text.

15 28. Search of the computer for the evidence described in Attachment B-1 may  
16 require a range of data analysis techniques. In some cases, agents may recover evidence  
17 with carefully targeted searches to locate evidence without requirement of a manual  
18 search through unrelated materials that may be commingled with criminal evidence.  
19 Agents may be able to execute a "keyword" search that searches through the files stored  
20 in a digital device for special terms that appear only in the materials covered by the  
21 warrant. Or, agents may be able to locate the materials covered by looking for a particular  
22 directory of file name. However, in other cases, such techniques may not yield the  
23 evidence described in the warrant. Individuals may mislabel or hide files and directories;  
24 encode communications to avoid using key words; attempt to delete files to evade  
25 detection; or take other steps designed to hide information from law enforcement  
26 searches for information.

27 29. The search procedure of any digital media seized may include the following  
28 on-site techniques to seize the evidence authorized by Attachment B-1:

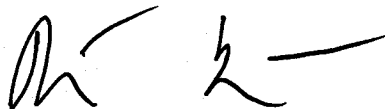
1 a. On-site triage of computer systems to determine what, if any,  
2 peripheral devices or digital storage units have been connected to such computer systems,  
3 a preliminary scan of image files contained on such systems and digital storage devices to  
4 help identify any other relevant evidence or potential victims or co-conspirators.

5 b. On-site copying and analysis of volatile memory, which is usually  
6 lost if a computer is powered down, and may contain information about how the  
7 computer is being used, by whom, when and may contain information about encryption,  
8 virtual machines, or stenography which will be lost if the computer is powered down.

9 c. On-site forensic imaging of any computers may be necessary for  
10 computers or devices that may be partially or fully encrypted in order to preserve  
11 unencrypted data that may, if not immediately imaged on-scene become encrypted and  
12 accordingly become unavailable for any examination.

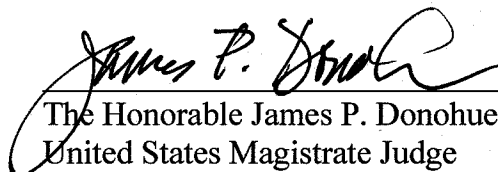
13 **CONCLUSION**

14 30. Based upon the evidence gathered in this investigation and set out above, I  
15 submit that there is probable cause to believe that the locations describe in Attachments A  
16 contain evidence of drug trafficking, and I seek permission to seize the items described in  
17 Attachments B.

18 

19 MICHAEL FISCHLIN, Affiant  
20 Inspector, USPIS

21  
22  
23 SUBSCRIBED AND SWORN before me on this 11<sup>th</sup> day of December, 2018.

24   
25 The Honorable James P. Donohue  
26 United States Magistrate Judge  
27  
28

**ATTACHMENT A-1**

**Place To Be Searched**

The place to be searched is 5834 NE 75th Street, apt B208, Seattle, WA 98115.

**ATTACHMENT A-2**

**Place To Be Searched**

The property to be searched is an Android phone, model 1+, phone number 206-316-6268, believed to belong to MATTHEW WITTERS.



**Attachment B-1**

This warrant authorizes the government to search for the following items that are evidence and/or fruits of possession of controlled substances with intent to distribute and/or distribution of controlled substances:

1. Any controlled substances, in particular fentanyl
2. Drug Paraphernalia: Items to be used to store and distribute controlled substances, such as plastic bags, cutting agents, scales, measuring and packaging equipment and similar items.
3. Drug Transaction Records: Documents such a ledgers, receipts, notes, books and similar items relating to the acquisition, and distribution of controlled substances, however stored, including in digital devices.
4. Customer Supplier Information: Items identifying drug customers and drug suppliers, such as address and/or telephone books, correspondence, diaries, calendars, notes with phone numbers and names, "pay/owe sheets" with drug amounts and prices, papers reflecting names, addresses, and/or telephone numbers of co-conspirators.
5. Documents reflecting the source, receipt, transfer, ownership and disposition of the United States Currency or other monetary instruments, of real estate and personal property, such as vehicle registration, insurance documents, account bank statements, registers, deposit tickets, concealed checks, loan paperwork, wire transfer receipts, debit and credit tickets, and correspondence.
6. All bank and financial records, including bank statements, wire transfers slips/orders, money order receipts, ATM receipts, cashier checks, cashier check receipts, and safe deposit records for the years 2014 through the present.
7. Rental Agreements, correspondence, keys and entry records for the safe deposit boxes and storage units.
8. Correspondence, papers, records, and any other items showing employment or lack thereof.
9. Records of domestic of domestic and foreign travel such as itineraries, passports, tickets, lodging receipts, and payment records.

10. Records an item identifying smart phones, telephones and pagers used by conspirators including telephone toll bills, pager bills, subscriber agreements, cellular telephones/smart phones and pagers.
11. All firearms and ammunition.
12. Items tending to establish the identity of persons in control of the premises or vehicle being searched.
13. For the Tower, ASUS model, v12xT,
  - a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;
  - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;
  - f. evidence of the times the digital device or other electronic storage media was used;
  - g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;
  - h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

- i. contextual information necessary to understand the evidence described in this attachment.
- j. all documents reflecting cryptocurrencies, including web history, and documents showing the location, source, and timing of acquisition, of any cryptocurrencies

THE SEIZURE OF THE COMPUTER DESCRIBED ABOVE IS AUTHORIZED FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATION OF ITS CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES

**ATTACHMENT B-2**

**Items to be Seized**

This warrant authorizes the government to search for the following items that are evidence and/or fruits of possession of controlled substances with intent to distribute and/or distribution of controlled substances:

- a. Assigned number and identifying telephone serial number (ESN, MIN, IMSI, or IMEI);
- b. Stored list of recent received, sent, and missed calls;
- c. Stored contact information;
- d. Stored photographs of narcotics, currency, firearms or other weapons, evidence of suspected criminal activity, and/or the user of the phone or suspected co-conspirators, including any embedded GPS data associated with those photographs;
- e. Stored text messages.
- f. digital currency applications and wallets, to include information regarding current balance and transaction history, *i.e.*, date, time, amount, and address of the sender/recipient of a digital currency transaction maintained in such wallets;

# Attachment C

1                                   **AFFIDAVIT OF MICHAEL FISCHLIN**

2   STATE OF WASHINGTON        )  
   )  
 3   COUNTY OF KING            )       ss  
 4

5           I, Michael Fischlin, an Inspector with United States Postal Inspection Service  
 6 ("USPIS"), Seattle, Washington, having been duly sworn, state as follows:

7                                   **INTRODUCTION AND AGENT BACKGROUND**

8           1.     I am a Postal Inspector with the USPIS and have been so employed since  
 9 June 2016. I am currently assigned to the Seattle Division, Prohibited Mail Narcotics  
 10 Team, where I investigate controlled substances transported via the United States Mail. I  
 11 have attended a one-week training course presented by the USPIS addressing narcotics  
 12 investigations and trends in narcotics mailings. At that training, subject matter experts  
 13 taught current trafficking trends and suspicious parcel recognition.

14          2.     Prior to becoming a Postal Inspector, I was employed as a Special Agent  
 15 ("SA") of the United States Secret Service ("USSS"). As part of my training, I  
 16 completed the Federal Law Enforcement Training Center ("FLETC") Criminal  
 17 Investigator Training Program as well as the USSS SA Training Program. While  
 18 employed by the USSS, I was trained in computer forensics. Prior to joining the USSS, I  
 19 served four years of active duty in the United States Marine Corps as a military  
 20 policeman.

21          3.     As a Postal Inspector, I am authorized to investigate crimes involving  
 22 federal offenses relating to the United States Postal Service ("USPS"). During the course  
 23 of my law enforcement career, I have conducted or participated in criminal investigations  
 24 involving access device fraud, bank fraud, computer fraud, counterfeit currency and  
 25 securities, identity theft, illegal narcotics, mail theft, robbery, and wire fraud. My duties  
 26 have included planning the execution of search warrants; securing and searching  
 27 premises; seizing documents, records and other evidence; and interviewing witnesses.



5. This affidavit is submitted in support of an application for a search and seizure warrant for the following property:

6. As set forth below, there is evidence that the SAFE DEPOSIT BOX contains evidence of drug trafficking, in violation of Title 21, United States Code, Section 841(a)(1), including conspiracy to distribute controlled substances, in violation of Title 21, United States Code, Section 846. I seek authority to seize the items described in Attachment B, which is incorporated herein by reference.

- a. Up to \$86,666.82 in U.S. funds contained in U.S. Bank account number X-XXX-XXXX-1982 held in the name of MATTHEW M. WITTERS ("WITTERS's Checking Account");
- b. Up to \$329,250.15 in U.S. funds contained in U.S. Bank account number X-XXX-XXXX-7643 held in the name of MATTHEW M. WITTERS ("WITTERS's Savings Account");

- c. Up to \$3,180 in U.S. funds contained in GBC International Bank account number XXXXX1014 held in the name of MATTHEW M. WITTERS ("WITTERS's GBC Savings Account");
- d. All funds, including cryptocurrencies, contained in any Gemini Trust Company accounts held in the name of MATTHEW WITTERS with Social Security Number XXX-XX-8436 ("WITTERS's Gemini Account");
- e. All funds, including cryptocurrencies, contained in any Bittrex accounts held in the name of MATTHEW WITTERS with date of birth XX/XX/1979 ("WITTERS's Bittrex Account"); and
- f. All U.S. dollar funds contained in Robinhood Markets, Inc. account number XXXX8546 held in the name of MATTHEW WITTERS ("WITTERS's Robinhood Account").

8. As set forth below, I submit that there is probable cause to believe that the SUBJECT ASSETS are property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of violations of 21 U.S.C. §§ 841(a)(1), (b)(1)(A), and 846 (conspiracy to distribute controlled substances), and/or are property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violations. The SUBJECT ASSETS are therefore subject to forfeiture to the United States under 21 U.S.C. § 853(a).

9. I further submit that there is probable cause to believe that the SUBJECT ASSETS constitute (1) moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished in exchange for a controlled substance, in violation of the Controlled Substances Act ("CSA"); (2) proceeds traceable to such an exchange; or (3) moneys, negotiable instruments, or securities used or intended to be used to facilitate a violation of the CSA. The SUBJECT ASSETS are therefore subject to forfeiture to the United States under 21 U.S.C. § 881(a)(6).

10. Because this affidavit is submitted for the limited purpose of obtaining search and seizure warrants, I am not including every fact known to me about WITTERS or the larger investigation.

#### **FORFEITURE AND SEIZURE AUTHORITY**

11. As to civil forfeiture, under 21 U.S.C. § 881(a)(6), “[t]he following shall be subject to forfeiture to the United States and no property right shall exist in them: . . . All moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished by any person in exchange for a controlled substance or listed chemical in violation of this subchapter, all proceeds traceable to such an exchange, and all moneys, negotiable instruments, and securities used or intended to be used to facilitate any violation of this subchapter.”

12. Property subject to civil forfeiture under 21 U.S.C. § 881(a) may be seized pursuant to 18 U.S.C. § 981(b) (by 21 U.S.C. § 881(b)).

13. As to criminal forfeiture, under 21 U.S.C. § 853(a), “[a]ny person convicted of a violation of this subchapter or subchapter II of this chapter punishable by imprisonment for more than one year shall forfeit to the United States, irrespective of any provision of State law [*inter alia*]—(1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; [and] (2) any of the person’s property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.”

14. Property subject to criminal forfeiture under 21 U.S.C. § 853 may be seized pursuant to 21 U.S.C. § 853(f). With respect to seizure, 21 U.S.C. § 853(f) specifically provides that a court may issue a criminal seizure warrant when it “determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a[] [protective] order under [21 U.S.C. § 853(e)] may not be sufficient to assure the availability of the property for forfeiture.”

15. Here, because the SUBJECT ASSETS may be easily withdrawn, transferred, dissipated, or otherwise made unavailable for forfeiture, a protective order

1 may not be sufficient to ensure that the SUBJECT ASSETS remain available for  
 2 forfeiture. For that reason, the United States seeks combined criminal and civil seizure  
 3 warrants, authorizing law enforcement to seize the SUBJECT ASSETS and preserve  
 4 them pending further forfeiture proceedings.

#### 5 **BACKGROUND ON THE DARK WEB AND CRYPTOCURRENCY**

6 16. Based on my training, research, education, and experience, I am familiar  
 7 with the following relevant terms and definitions:

8 a. The "dark web" is a portion of the "Deep Web"<sup>1</sup> of the Internet,  
 9 where individuals must use anonymizing software or applications to access content and  
 10 websites. Within the dark web, criminal marketplaces operate, allowing individuals to  
 11 buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with  
 12 greater anonymity than is possible on the traditional Internet (sometimes called the "clear  
 13 web" or simply the "web"). These online market websites use a variety of technologies,  
 14 including the Tor network (defined below) and other encryption technologies, to ensure  
 15 that communications and transactions are shielded from interception and monitoring.  
 16 Famous dark web marketplaces, also called Hidden Services, such as Silk Road,  
 17 AlphaBay,<sup>2</sup> and Dream Market,<sup>3</sup> operate(d) similarly to clear web commercial websites  
 18 such as Amazon and eBay, but offered illicit goods and services.

19 b. "Vendors" are the dark web's sellers of goods and services, often of  
 20 an illicit nature, and they do so through the creation and operation of "vendor accounts"  
 21 on dark web marketplaces. Customers, meanwhile, operate "customer accounts." Vendor  
 22 and customer accounts are not identified by numbers, but rather monikers or "handles,"  
 23  
 24

25 <sup>1</sup> The Deep Web is the portion of the Internet not indexed by search engines. Examples are databases and  
 26 internal networks belonging to private industry, government agencies, or academic institutions.

27 <sup>2</sup> Based upon my training and experience, I know that AlphaBay was a website on the dark web that  
 28 offered drugs and other contraband for sale. Furthermore, I know that AlphaBay was seized by U.S. law  
 enforcement in July 2017.

<sup>3</sup> Based upon my training and experience, I know that Dream Market is a website on the dark web that  
 offers drugs and other contraband for sale.

1 much like the username one would use on a clear web site. If a moniker on a particular  
2 marketplace has not already been registered by another user, vendors and customers can  
3 use the same moniker across multiple marketplaces, and based on seller and customer  
4 reviews, can become well known as "trusted" vendors or customers. It is also possible  
5 for the same person to operate multiple customer accounts and multiple vendor accounts  
6 at the same time. For example, based on my training and experience, I know that one  
7 person could have a vendor account that he or she uses to sell illegal goods on a dark web  
8 marketplace in exchange for cryptocurrency; that same vendor could also have a different  
9 customer account that he or she uses to exchange cryptocurrency earned from vendor  
10 sales for fiat currency.<sup>4</sup> Because they are separate accounts, a person could use different  
11 accounts to send and receive the same cryptocurrency on the dark web. I know from  
12 training and experience that one of the reasons dark web vendors have multiple monikers  
13 for different vendor and customer accounts is to prevent law enforcement from  
14 identifying which accounts belong to the same person and who the actual person is that  
15 owns or uses the accounts.

16 c. Pretty Good Privacy ("PGP") is used on dark web markets to encrypt  
17 communications between vendors and customers. When a customer orders from a  
18 vendor or sends a vendor a message on a dark web market, that information may be  
19 stored in the marketplace's database. Given concerns that the marketplace server may be  
20 hacked or seized by law enforcement, vendors and customers often communicate via  
21 PGP-encrypted means to address this security problem.

22 d. The "Tor network," or simply "Tor," (an abbreviation for "The  
23 Onion Router") is a special network of computers on the Internet, distributed around the  
24 world, designed to conceal the true Internet Protocol ("IP") addresses of the computers  
25 accessing the network, and, thereby, the locations and identities of the network's users.

26  
27 <sup>4</sup> Fiat currency is currency created and regulated by a government such as the U.S. Dollar, Euro, or  
28 Japanese Yen.

1 Tor also enables websites to operate on the network in a way that conceals the true IP  
 2 addresses of the computer servers hosting the websites, which are referred to as "hidden  
 3 services" on the Tor network. Such hidden services operating on Tor have complex web  
 4 addresses, generated by a computer algorithm, ending in ".onion" and can only be  
 5 accessed through specific web browser software, including a browser known as "Tor  
 6 Browser," designed to access the Tor network. An example of a hidden services website  
 7 is the aforementioned AlphaBay.

8 e. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to  
 9 peer, network-based medium of value or exchange that may be used as a substitute for  
 10 fiat currency to buy goods or services or exchanged for fiat currency or other  
 11 cryptocurrencies. Examples of cryptocurrency are Bitcoin<sup>5</sup> ("BTC"), Ethereum ("ETH"  
 12 or "ether"), and Tether ("USDT"). Cryptocurrency can exist digitally on the Internet, in  
 13 an electronic storage device, or in cloud-based servers. Although not usually stored in  
 14 any physical form, public and private keys (described below) used to transfer  
 15 cryptocurrency from one person or place to another can be printed or written on a piece  
 16 of paper or other tangible object. Cryptocurrency can be exchanged directly person to  
 17 person, through a cryptocurrency exchange, or through other intermediaries. Generally,  
 18 cryptocurrency is not issued by any government, bank, or company; it is instead  
 19 generated and controlled through computer software operating on a decentralized peer-to-  
 20 peer network. Most cryptocurrencies have a "blockchain," which is a distributed public  
 21 ledger, run by the decentralized network, containing an immutable and historical record  
 22 of every transaction.<sup>6</sup> Cryptocurrency is not illegal in the United States.

23  
 24  
 25 <sup>5</sup> Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use  
 26 "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and  
 27 "bitcoin" (with a lowercase letter b) or "BTC" to label units of the cryptocurrency. That practice is  
 28 adopted here.

<sup>6</sup> Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate  
 transactions, making it difficult to trace or attribute transactions.



1 f. Bitcoin is a type of cryptocurrency. Payments or transfers of value  
2 made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by  
3 any single administrator or entity. As mentioned above, individuals can acquire bitcoin  
4 through exchanges (i.e., online companies which allow individuals to purchase or sell  
5 cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin  
6 ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by  
7 "mining." An individual can "mine" bitcoins by using his/her computing power to solve  
8 a complicated algorithm and verify and record payments on the blockchain. Individuals  
9 are rewarded for this task by receiving newly created units of a cryptocurrency.  
10 Individuals can send and receive cryptocurrencies online using many types of electronic  
11 devices, including laptop computers and smart phones. Even though the public addresses  
12 of those engaging in cryptocurrency transactions are recorded on a blockchain, the  
13 identities of the individuals or entities behind the public addresses are not recorded on  
14 these public ledgers. If, however, an individual or entity is linked to a public address, it  
15 may be possible to determine what transactions were conducted by that individual or  
16 entity. Bitcoin transactions are therefore sometimes described as "pseudonymous,"  
17 meaning that they are partially anonymous. And while it is not completely anonymous,  
18 Bitcoin allows users to transfer funds more anonymously than would be possible through  
19 traditional banking and credit systems.

20 g. Cryptocurrency is stored in a virtual account called a wallet. Wallets  
21 are software programs that interface with blockchains and generate and/or store public  
22 and private keys used to send and receive cryptocurrency. A public key (or public  
23 address) is akin to a bank account number, and a private key (or private address) is akin  
24 to a Personal Identification Number ("PIN") number or password that allows a user the  
25 ability to access and transfer value associated with the public address or key. To conduct  
26 transactions on a blockchain, an individual must use the public key and the private key.  
27 A public address is represented as a case-sensitive string of letters and numbers. Each  
28 public address is controlled and/or accessed through the use of a unique corresponding

1 private key—the cryptographic equivalent of a password or PIN—needed to access the  
 2 address. Only the holder of an address's private key can authorize any transfers of  
 3 cryptocurrency from that address to another cryptocurrency address.

4 h. Although cryptocurrencies such as Bitcoin have legitimate uses,  
 5 cryptocurrency is also used by individuals and organizations for criminal purposes such  
 6 as money laundering, and is an oft-used means of payment for illegal goods and services  
 7 on hidden services websites operating on the Tor network. By maintaining multiple  
 8 wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law  
 9 enforcement's efforts to track purchases within the dark web marketplaces. As of  
 10 December 3, 2018, one bitcoin is worth approximately \$3,818.15, though the value of  
 11 bitcoin is generally much more volatile than that of fiat currencies.

12 i. Exchangers and users of cryptocurrencies store and transact their  
 13 cryptocurrency in a number of ways, as wallet software can be housed in a variety of  
 14 forms, including: on a tangible, external device ("hardware wallet"); downloaded on a  
 15 Personal Computer ("PC") or laptop ("desktop wallet"); with an Internet-based cloud  
 16 storage provider ("online wallet"); as a mobile application on a smartphone or tablet  
 17 ("mobile wallet"); as printed public and private keys ("paper wallet"); and as an online  
 18 account associated with a cryptocurrency exchange. Because these desktop, mobile, and  
 19 online wallets are electronic in nature, they are located on mobile devices (e.g., smart  
 20 phones or tablets) or at websites that users can access via a computer, smart phone, or any  
 21 device that can search the Internet. Moreover, hardware wallets are located on some type  
 22 of external or removable media device, such as a Universal Serial Bus ("USB") thumb  
 23 drive or other commercially available device designed to store cryptocurrency (e.g.  
 24 Trezor, Keepkey, or Nano Ledger). In addition, paper wallets may contain an address  
 25 and a QR code<sup>7</sup> with the public and private key embedded in the code. Paper wallet keys  
 26 are not stored digitally. Wallets can also be backed up into, for example, paper printouts,  
 27

28 <sup>7</sup> A QR code is a matrix barcode that is a machine-readable optical label.  
 Affidavit of Inspector Fischlin - 9  
 USAO#2017RO1197

1 USB drives, or CDs, and accessed through a "recovery seed" (random words strung  
2 together in a phrase) or a complex password. Additional security safeguards for  
3 cryptocurrency wallets can include two-factor authorization (such as a password and a  
4 phrase). I also know that individuals possessing cryptocurrencies often have safeguards  
5 in place to ensure that their cryptocurrencies become further secured in the event that  
6 their assets become potentially vulnerable to seizure and/or unauthorized transfer.

7 j. Cryptocurrency mixing services exist which allow for a user to make  
8 their transactions and digital assets anonymous on the blockchain. Cryptocurrency  
9 mixing services work by sending a user's coins to a pool where they are then mixed with  
10 coins belonging to others. A user then receives coins from wallets that are unrelated to  
11 their own, thereby obfuscating the link between a user's old and new wallets. These  
12 services are often referred to as a "mixers" or "tumblers."<sup>8</sup>

13 k. Bittrex, Coinbase, and Gemini Trust Company ("Gemini") are  
14 companies that each offer a cryptocurrency wallet service. Users of Bittrex, Coinbase,  
15 and Gemini can create online accounts with the respective companies where they can  
16 purchase, sell, exchange, store, receive, and/or transfer cryptocurrencies.

17 l. According to its website, Gemini is a digital asset exchange that  
18 allows users to buy, sell, and store digital assets such as bitcoins. According to its  
19 website, Bittrex is a blockchain platform that provides users with digital wallets and the  
20 ability to execute trades.

21 m. In light of the above information regarding Bittrex and Gemini, I  
22 anticipate that both companies, if served with a seizure warrant, would be capable of  
23 assisting with the seizure of cryptocurrencies that are stored in, or accessible via, Bittrex  
24 and Gemini-provided wallets.

25  
26  
27  
28 <sup>8</sup> Based upon my training and experience, I know that dark web vendors often utilize mixers allowing  
them to transact anonymously on the blockchain.

### SUMMARY OF PROBABLE CAUSE

### A. The Seized Packages

17. During the investigation, law enforcement seized multiple packages of drugs that were destined for WITTERS.

18. Specifically, on or about November 20, 2017, I intercepted an international parcel at the Shoreline Post office. The parcel was from China and addressed to WITTERS at 16738 2nd Ave NE, Shoreline, WA. A Homeland Security Investigations ("HSI") SA conducted an extended border search of the parcel. The parcel contained small plastic baggies with a white powder and a rock-like substance. The substances found within the parcel were sent to the Washington State Patrol ("WSP") Crime Laboratory for analysis. On November 27, 2018, the WSP Crime Laboratory provided results. Based upon gas chromatography/mass spectrometry and infrared spectroscopy, a WSP Crime Laboratory forensic scientist concluded that one of the baggies containing five grams of white powder contained fentanyl. USPS business records showed that a phone number associated with WITTERS had tracked the parcel.

19. On or about November 20, 2017, U.S. Customs and Border Protection ("CBP") in San Francisco, California, had seized an international parcel from China addressed to WITTERS at the same Shoreline address. The package contained a variety of substances, including approximately five grams of a substance that was presumptively identified as fentanyl hydrochloride. Fentanyl hydrochloride is the hydrochloride salt form of fentanyl.

20. Previously, on or about September 9, 2017, CBP in Torrance, California, had seized an international parcel from Tonga addressed to WITTERS at the same Shoreline address. The package contained a variety of substances, including approximately six grams of a substance that was presumptively identified as benzylfentanyl. Benzylfentanyl is a fentanyl analog.

1 **B. WITTERS's Orders on the Dark Web**

2 21. In April 2017, federal agents executed a search warrant for a residence in  
3 Oklahoma. The residence was associated with a dark web vendor who operated on  
4 AlphaBay who shipped controlled substances, including fentanyl, via the USPS. Agents  
5 seized drugs from the residence, including fentanyl. In addition, a spiral notebook was  
6 found inside of a backpack within the residence. One of the pages within the notebook  
7 contained a label bearing the name "Matt Witters" and the address "2104 SW 110th St,  
8 Seattle, WA 98146." On the same page, the word "saynotocustoms" was handwritten.  
9 Using a law enforcement database, I found that WITTERS was associated with this street  
10 address.

11 22. In December 2017, I learned of a USPIIS case in California that involved a  
12 suspect in Seattle. Specifically, in August 2017, S.G. was charged in the Southern  
13 District of California with Conspiracy to Distribute Fentanyl, Possession with Intent to  
14 Distribute Carfentanil, and Possession with Intent to Distribute Ketamine. Pursuant to a  
15 search warrant served on S.G.'s computers and investigation into S.G.'s dark web  
16 identities, it was determined that S.G. had operated on numerous dark web marketplaces,  
17 including AlphaBay. The investigation revealed that S.G. had completed thousands of  
18 transactions on the dark web where S.G. had bought and sold controlled substances  
19 throughout the United States. The investigation also revealed that S.G. imported  
20 narcotics into the United States.

21 23. A sales ledger was found on S.G.'s computer with entries listing the type  
22 and amount of drug sold, the buyer's dark web marketplace moniker, and the name and  
23 address of where the package was sent. Two of the entries included WITTERS's name:

24 DEC 21  
25 Matt Witters – 1 K – sayNotoCustoms – Ab  
26 7905 Detroit Ave. SW  
27 Seattle, WA 98106-1906  
28

1 JUN 17

2 Matt Witters – 2 K – sayNotoCustoms

3 2104 SW 110<sup>th</sup> St.

4 Seattle, WA 98146

5 24. Using a law enforcement database, I found that WITTERS was associated  
6 with both of these street addresses. S.G. told law enforcement agents that “K” on the  
7 ledger referred to Ketamine. Ketamine is a Schedule III controlled substance.

8 **C. sayNOtoCUSTOMS’s Dream Market Profile**

9 25. As discussed above, the phrase “saynotocustoms” was found on the spiral  
10 notebook in S.G.’s residence. On or about August 22, 2017, USPIS Inspector Brett  
11 Willyerd and I located the vendor profile for “sayNOtoCUSTOMS” on Dream Market, a  
12 dark web marketplace.<sup>9</sup> The profile picture for sayNOtoCUSTOMS was of Homer  
13 Simpson wearing a reggae hat and glasses. At that time, sayNOtoCUSTOMS was in  
14 “vacation mode,” meaning that sayNOtoCUSTOMS was not actively taking new orders  
15 for narcotics via Dream Market. However, Dream Market showed that  
16 sayNOtoCUSTOMS’s last active date was on or about August 22, 2017, meaning that  
17 someone had logged into the account on that day.

18 26. On or about October 6, 2017, I viewed sayNOtoCUSTOMS’s profile on  
19 Dream Market. sayNOtoCUSTOMS was no longer in vacation mode. The following  
20 comment was under the terms and conditions of sayNOtoCUSTOMS’s profile:

21 BACK from vacation. If my listings are up I am working and  
22 you will get it in timely manner, you never have to ask. I  
23 ALWAYS take my listings down when I’m not gonna be  
24 working. If you’ve ordered and haven’t received it and I take  
25 my listings down and put my status on vacation rest assured  
26 your stuff is coming.

27 <sup>9</sup> The moniker “sayNOtoCUSTOMS” appeared on multiple dark web sites and in various other places,  
28 often with different letters capitalized. For ease of reference, this Affidavit uses a single form of  
capitalization of the moniker.



27. I observed that sayNOtoCUSTOMS had three separate listings for fentanyl, varying from 500 milligrams to 3 grams. sayNOtoCUSTOMS indicated that orders of 500 milligrams and under would be shipped via first-class mail. I reviewed a listing for 1 gram of fentanyl and observed that the only shipping option was priority mail. I also observed a comment under the terms and conditions of sayNOtoCUSTOMS's profile regarding the need for customers to use Kleopatra. Kleopatra is an application used to store PGP certificates and keys.

28. On or about November 8, 2017, I viewed sayNOtoCUSTOMS's profile on Dream Market. I observed four separate listings for fentanyl, varying from 250 milligrams to 3 grams. Under the terms and conditions section of the profile, I observed the following: "UPDATE 11/2: I'm not retiring afterall... I had a massive loss of money so I need to work still... despite the major risks. I'm trying to find a partner to ship for me but rn im doing it." I also noticed another update: "UPDATE 10/27: I had some life situation pop up this week that required my full attention ad a few packs went out late. You guys know for 3 yrs I've been the fastest guy anywhere, but life happens, There might be a 3-4 day delay for a few of your orders this week. sorry guys, remember I'm not amazon."

29. On or about November 15, 2017, I viewed sayNOtoCUSTOMS's profile on Dream Market. I observed nine separate listings for fentanyl, six of which were for nasal sprays. A 500 milligram fentanyl listing by sayNOtoCUSTOMS contained the following under the shipping and refunds section of the product description:

So due to security and shipping concerns (the bulk of orders are under 500mg, and having giant bags of parcels is a red flag), everything up to 500mg will be shipping using first class mail now, 1g and up will go priority with tracking, first class mail letters will be UNTRACKED and you agree that if your order is lost there will be NO RESHIPS on any orders up to 500mg, this is just the chance you gotta take if you wanna order from me. I haven't had a parcel be lost in a long time, as long as the address you give me is correct and valid.

1 If your order is 500mg and below make sure you are able to  
2 get your mail daily and check for your letter.

3 30. In addition, under sayNOtoCUSTOMS's listings for fentanyl spray there  
4 was a product description, which included: "I sold thousands of these on Alpahbay. You  
5 can carry them around anywhere you go and take your meds when and where you need  
6 them, anyone looking thinks you just have allergies! I've literally done sprays RIGHT  
7 next to a cop in line at the grocery store. Who would know? no one."

8 31. In addition to the fentanyl listings, there was a listing titled "REAL  
9 ALPLAX 2MG BARS BY GADOR PHARMA!" The listing included a photograph of  
10 numerous white strips of tablets laid on a black surface. Alplax is also know by the brand  
11 name Xanax, and contains the drug alprazolam, which is a Schedule IV controlled  
12 substance.

13 32. On or about November 17, 2017, I accessed Dream Market. I was unable  
14 to find any listings by sayNOtoCUSTOMS.

15 33. On or about February 2, 2018, I logged into Dream Market and viewed  
16 sayNOtoCUSTOMS's profile. Dream Market showed that sayNOtoCUSTOMS had  
17 retired on November 26, 2017. Under the terms and conditions section of the profile, I  
18 observed the following: "11/17; On vacation sorry guys don't know for how long, could  
19 be a long time. all orders went out that were accepted, one i accepted and then rejected.  
20 Sorry guys, it is what it is."

21 34. Dream Market showed that sayNOtoCUSTOMS joined on November 13,  
22 2015. sayNOtoCUSTOMS had 340 reviews with an overall rating of 4.92 out of 5. Due  
23 to my experience, I know that a review is generally associated with an order, meaning  
24 that sayNOtoCUSTOMS had conducted at least 340 orders on Dream Market. During  
25 my reviews of the account, I observed that sayNOtoCUSTOMS had sold both fentanyl  
26 and Xanax. Fentanyl was sold in the form of both a powder and a nasal spray.

**D. sayNOtoCUSTOMS's Profile on AlphaBay**

35. sayNOtoCUSTOMS also operated on AlphaBay, which, as described above, was a dark web marketplace that was seized by law enforcement in July 2017. I reviewed records from the seized AlphaBay server, which contained information about the vendor account for sayNOtoCUSTOMS. The profile picture for the account was of Homer Simpson wearing a reggae hat and glasses, which matched the profile picture for sayNOtoCUSTOMS on Dream Market.

36. The sayNOtoCUSTOMS profile included an "about" section which began: "I'm a real fentanyl HCL vendor (pure 98% fully water soluble salts), not the bullshit analogs." Records showed that sayNOtoCUSTOMS sold fentanyl and Xanax on the marketplace. Fentanyl was sold in the form of both a powder and a nasal spray.

37. A review of the AlphaBay records revealed a listing by sayNOtoCUSTOMS titled "800 REAL ALPLAX BRAND BARS BY GADOR PHARMACEUTICAL - USA." The listing included a photograph of numerous white strips of tablets laid on a black surface. The photograph matched the photograph for a similar listing by sayNOtoCUSTOMS on Dream Market, providing further evidence that sayNOtoCUSTOMS was controlled by the same user on both Dream Market and AlphaBay.

38. Records showed that sayNOtoCUSTOMS registered on AlphaBay on or about November 8, 2015. sayNOtoCUSTOMS was last active on the site on or about July 5, 2017. sayNOtoCUSTOMS completed approximately 2,383 orders. Records indicated that, from around November 2015 to July 2017, sayNOtoCUSTOMS received approximately 1,165 bitcoins as payment for the orders.

39. Records further showed that sayNOtoCUSTOMS posted a message on AlphaBay Market Forum regarding the use of a mixer to anonymize coins withdrawn from AlphaBay. The message included the following:

Thats great, so I have been using bitblender<sup>10</sup> for my blending. has anyone checked how effective AB's tumbling is? I'm not hip enough to figure out if w/d's strait from AB are fully untraceable or is it possible to see the coins came from AB unless you tumble them a second time? i think .5% is more than fair for simple computer operation. So I'm a level 6 vendor with 3k a day in sales. should I tumble them still or should I be safe with AB's new tech?

**E. Related Vendor Account on AlphaBay**

40. As discussed below, the vendor account "kakashisan" on AlphaBay appeared to be controlled by the same user as sayNOtoCUSTOMS.

41. I reviewed the seized AlphaBay server for records pertaining to kakashisan. The records showed that kakashisan registered on AlphaBay on or about September 20, 2015. kakashisan was last active on the site on or about July 1, 2017. kakashisan completed approximately 215 orders for approximately 106 bitcoins. kakashisan sold fentanyl and Xanax on the marketplace. Fentanyl was sold in the form of both a powder and a nasal spray.

42. Records showed kakashisan posted a message on the AlphaBay Market Forum claiming to reside in Seattle. On November 1, 2015, kakashisan also posted a message advising that he had created a new account under the name sayNOtoCUSTOMS which read:

I finally got my hands on a few hundred real Alplax bbrand bars by Gador pharmaceuticals (I always put alprax cause i buy those too sometimes from an indian seller and i get the names mixed up lol, these are alplax bars by gador), they are hands down the best quality xanax bar on the planet. Don't believe me? google it. I'm 100% sure I'm the only human on early selling these us to us on any market. enjoy :) i only got 400 of them but they are worth every penny, the champagne of bars lol.

<sup>10</sup> Based upon my training and experience, I know that Bitcoin Blender is a Tor hidden service that allows users to obfuscate their Bitcoin transactions.

1 I've made a new account and will be listing them on Sunday  
2 11/7 under the account sayNOtoCUSTOMS

3 43. A message from the AlphaBay server that was sent by sayNOtoCUSTOMS  
4 on November 18, 2015, further indicated that sayNOtoCUSTOMS and kakashisan were  
5 controlled by the same person. The message was titled, "Whoops! This is kakashisan!"  
6 and included the following: "I forgot to tell you that I made this account for my vending  
7 now I started vending on kakashisan and decided it was smarter to have a separate vend  
8 account."

9 44. In another message that was part of the same exchange,  
10 sayNOtoCUSTOMS wrote:

11 please I've given plenty of proof this is my account, look at  
12 my post in november that says "This is kakashisan!" cause  
13 people were getting confused, please guys i've been of or  
14 your top vendors for a long time almost 600k in sales please  
15 you KNOW it's me. Its my commission account. I'm a good  
16 vendor people really like me can you please just do this one  
17 favor for me?

18 **F. WITTERS's Ties to sayNOtoCUSTOMS and kakashisan**

19 45. During my investigation, I uncovered numerous pieces of evidence tying  
20 WITTERS to the sayNOtoCUSTOMS and kakashisan accounts. First, according to the  
21 seized AlphaBay records, the date of birth associated with the sayNOtoCUSTOMS and  
22 kakashisan profiles matched WITTERS's date of birth.

23 46. Second, as detailed above, S.G.'s drug ledger indicated that  
24 sayNOtoCUSTOMS was WITTERS.

25 47. Third, USPS business records showed several USPS accounts in  
26 WITTERS's name. One of the accounts listed an address of 7905 Detroit Ave SW,  
27 Seattle, WA. The account had a user name of "kakashisan." It should be noted the  
28 address for this account matched one of the addresses for WITTERS listed on S.G.'s drug  
ledger.

1 48. Fourth, the email address associated with sayNOtoCUSTOMS on Dream  
 2 Market was anon432112344321@gmail.com. I obtained a search warrant for this  
 3 account and it contained several emails indicating that WITTERS had control over the  
 4 email account. For example, I located an email sent on February 18, 2016, regarding an  
 5 order for Alprax in which MoneyGram was used for payment that included the following  
 6 message:

7 Hey bud I just sent moneygram for \$660 for 100 viagra and  
 8 1000 alprax. \$150 for the viagra and \$500 for the alprax and  
 9 \$10 shipping.

10 Sent to: USARAK PUTTAWONG

11 Senders name: MATTHEW WITTERS

12 Senders City: Seattle, WASHINGTON, USA

13 49. I located another email sent by anon432112344321@gmail.com on April  
 14 15, 2016, in which the user provided a name and address for shipment. The name and  
 15 address provided was Matt WITTERS, 7905 Detroit Ave SW, Seattle, WA 98106.

16 50. Fifth, I also located in this email account a message in which the user  
 17 shared the PGP public key for kakashisan and otherwise referred to that vendor name and  
 18 sayNOtoCUSTOMS. Specifically, the message, send on November 9, 2015, stated:

19 here is kakashisan's pgp again. I have a new vendor account  
 20 on alphabay called "sayNOtoCUSTOMS" I'll give you that  
 21 pgp too. please import both pgp certificates to your pgp.  
 22 Kakshisan PGP, this is for SURE the same pgp as i used on  
 23 abraxas [i.e., a different dark net drug market].

24 51. In addition, I located in the email account a message containing the PGP  
 25 public key for sayNOtoCUSTOMS. The message stated: "new PGP for my vendor  
 26 account called sayNOtoCUSTOMS." I also located in the email account a message  
 27 addressed to the user of the account that began, "Hi saynotocustoms".

28 52. Sixth, I obtained an email search warrant for a different email account  
 associated with WITTERS, cssrules@gmail.com, which contained additional evidence.  
 For example, I recovered an email with an attached photograph of WITTERS holding his



1 driver's license and a piece of paper that said, "cryptsy - 11/24/2015" under which  
2 "kakashisan" was written. I also located an email with an attached photograph of  
3 numerous white strips of tablets laid on a black surface. The photograph matched the  
4 photograph for the sayNOtoCUSTOMS Alplax listings on both AlphaBay and Dream  
5 Market. I also located an email sent by cssrules@gmail.com attached to which were the  
6 PGP private and public keys for kakashisan. The public PGP key matched the public  
7 PGP key found on the seized AlphaBay server for the vendor kakashisan. I also located  
8 numerous emails pertaining to orders for equipment and supplies that could be used in the  
9 distribution of controlled substances via the U.S. mail. The orders included such items as  
10 digital scales, heat/vacuum sealers, Mylar bags, plastic baggies, nasal spray bottles,  
11 bottles with droppers, printer ink cartridges, and mailing/shipping labels. In addition,  
12 numerous emails were located pertaining to USPS orders shipped to WITTERS for large  
13 quantities of priority mail boxes, priority mail envelopes, address labels, tracking labels,  
14 and stamps.

15 53. Seventh, WITTERS is closely associated with Bitcoin, a cryptocurrency  
16 used to conduct drug sales on Dream Market and AlphaBay. For example, WITTERS's  
17 Facebook account included a post responding to a post that showed a picture of cash.  
18 WITTERS posted:

19 That looks like 25k. I win lol, nah, cash is for suckers, buy  
20 bitcoin man. Cash aint gonna be worth the paper it's printed  
21 on soon. I wish I could buy a house with bitcoin but one day  
22 you will be able to. crypto is gonna get us out from under the  
23 banksters thumbs and we will truly be free. The age of  
information will bring about the age of empire.

24 54. Eighth, WITTERS on his Facebook page described losing a large amount  
25 of bitcoins, coinciding with the time that sayNOtoCUSTOMS went dark on Dream  
26 Market, explaining why he was no longer active on the dark web site. Specifically,  
27 WITTERS posted on Facebook on November 17, 2017:



1 if you guys would have bought bitcoin in september when it  
 2 crashed to 3kk cause china banned it (for the third time, they  
 3 will be unbanning it again here soon). btc hit 8k 3 times in  
 4 the last few days. I told you guys at \$400, \$650, \$800, etc, I  
 5 have the FB posts right here lol, you guys cant say you didn't  
 6 know. had a super bad week i got phished like an udiot and  
 7 lost 600k bitcoin, almost offed myself, then I remembered I  
 8 had 114 coins in an old blockchain wallet i forgot the pw to in  
 9 may 2016, i pestered blockchain.com, a company that offers  
 10 wallets, they had told me that if I lost my recovery phrase and  
 11 had second pw I was SOL, but i was looking around about it  
 12 online and fiund a post a guy nade of an email from  
 13 blockchain with an attachment of all his wallet backups, I was  
 14 like wtf, why shouldn't I be able to get my old wallet backup  
 emaild to me. They did it after pestering them for 2 days lol,  
 It was hard too I hade to figure out how top get my private  
 keys from the wallet it was nuts for days I sat here in the  
 hopes this would work and last night I did it I got 114 bitcoins  
 woth about 850k lol, sucks I got hacked but i prolyl never  
 would have gotten that wallet back if I wasn't desperate lol.

15 55. As noted above, sayNOtoCUSTOMS left Dream Market on or about  
 16 November 26, 2017, posting on November 17, 2017, the day of the Facebook post above:  
 17 "11/17; On vacation sorry guys don't know for how long, could be a long time. all orders  
 18 went out that were accepted, one i accepted and then rejected. Sorry guys, it is what it is."

19 **G. WITTERS's Accounts**

20 **L. Witters's U.S. Bank Accounts**

21 56. According to records obtained from U.S. Bank, WITTERS opened a  
 22 checking account (-1982) (i.e., WITTERS's Checking Account) in December 2015 and a  
 23 savings account (-7643) (i.e., WITTERS's Savings Account) in March 2018.

24 **1. WITTERS's Checking Account**

25 57. WITTERS's Checking Account is largely funded by electronic deposits  
 26 from the digital currency exchanges Coinbase and Gemini, as well as cash deposits.  
 27 Specifically, from December 2015 to October 2018, a total of approximately \$871,438.67  
 28 was deposited into WITTERS's Checking Account—of which, approximately

1 \$810,742.31 was received from Coinbase and Gemini, while \$14,780 was deposited in  
 2 the form of cash (as detailed below). It should be noted that WITTERS's Checking  
 3 Account was opened shortly after "kakashisan" and "sayNOtoCUSTOMS" began selling  
 4 controlled substances on AlphaBay.

5 58. The deposits from Coinbase and Gemini into WITTERS's Checking  
 6 Account include the following:

Date <sup>11</sup>	Depositing Institution	Amount
12/22/15	Coinbase	\$2,000
1/26/16	Coinbase	\$3,000
3/7/16	Coinbase	\$2,000
3/29/16	Coinbase	\$891.35
6/24/16	Coinbase	\$2,290
11/30/17	Gemini	\$9,000
12/19/17	Gemini	\$100,000
12/21/17	Gemini	\$100,000
12/22/17	Gemini	\$100,000
12/27/17	Gemini	\$100,000
12/28/17	Gemini	\$100,000
1/9/18	Gemini	\$100,000
1/16/18	Gemini	\$100,000
1/17/18	Gemini	\$91,560.96
	<b>Total =</b>	<b>\$810,742.31</b>

11 The dates listed are those included on WITTERS' U.S. Bank statements. The actual deposit date may predate the date listed.

59. Records from Coinbase revealed an account in WITTERS's name that had transacted in approximately 301 bitcoins. Records revealed at least two bitcoin wallet addresses provided by sayNOtoCUSTOMS on AlphaBay for withdrawal purposes resolved to the Coinbase account in WITTERS's name. Furthermore, records from Coinbase contained a note that WITTERS's account was associated with a high volume of dark web market activity and specifically listed AlphaBay. Based on my training and experience, I submit that this information demonstrates that WITTERS's Coinbase account was directly linked to dark web narcotics proceeds.

60. WITTERS's Checking Account is also funded by cash deposits. These cash deposits, which cumulatively amount to more than approximately \$14,780, include the following:

Date	Amount
12/18/15	\$200
4/5/16	\$2,000
4/12/16	\$1,620
1/2/17	\$420
1/3/17	\$2,000
1/20/17	\$6,000
3/20/17	\$1,340
6/17/17	\$200
6/23/17	\$1,000
<b>Total =</b>	<b>\$14,780</b>

61. As of October 9, 2018, WITTERS's Checking Account held a balance of approximately \$132,583.18.

1                   2.     WITTERS's Savings Account

2           62.     WITTERS's Savings Account was solely funded by a \$500,000 electronic  
3 transfer from WITTERS's checking account on or about March 15, 2018.

4           63.     As of October 24, 2018, WITTERS's Savings Account held a balance of  
5 approximately \$329,250.15. As described further below, the remaining approximately  
6 \$170,000 (of the \$500,000 transfer noted in the paragraph above) was transferred to  
7 another account held in WITTERS's name.

8           **II.     WITTERS's GBC Account**

9           64.     According to records obtained from GBC International Bank, WITTERS  
10 opened a savings account (-1014) (i.e., WITTERS's GBC Savings Account) in May  
11 2017. WITTERS's GBC Savings Account was funded entirely by cash deposits. These  
12 cash deposits include the following:

Date	Amount
5/17/17	\$900
7/21/17	\$1,000
8/31/17	\$680
9/21/17	\$600
<b>Total =</b>	<b>\$3,180</b>

13  
14  
15  
16  
17  
18  
19  
20           65.     As of December 3, 2018, WITTERS's GBC Savings Account held a  
21 balance of approximately \$3,860.69.

22           66.     WITTERS also holds the SAFE DEPOSIT BOX at GBC International  
23 Bank. On or about November 7, 2017, an HSI SA interviewed employees at the bank in  
24 Shoreline, WA. Several employees stated that WITTERS was observed bringing in  
25 bundles of U.S. currency to put into the SAFE DEPOSIT BOX. WITTERS told  
26 employees he made the money from bitcoin.

27           67.     On or about November 13, 2018, an HSI SA interviewed employees at the  
28 bank again. An employee confirmed that WITTERS is still the lessee of the SAFE

1 DEPOSIT BOX. An employee witnessed WITTERS access the SAFE DEPOSIT BOX  
 2 with bundles of currency in a bag and then come out without the bag. An employee  
 3 indicated that WITTERS openly spoke about how much money he made with bitcoin.  
 4 An employee advised that the SAFE DEPOSIT BOX was last accessed in March 2018.

5 68. I know based on my training and experience working narcotics cases that  
 6 drug dealers often use safe deposit boxes to hide valuables and the proceeds of their illicit  
 7 activities. The placement of these items in these locations serves to protect these items  
 8 from theft, as well as from potential seizure should law enforcement execute a search  
 9 warrant at the drug trafficker's primary residence.

10 69. I also know that persons involved in the trafficking of illicit drugs often keep  
 11 large amounts of cash either on hand, on their person, within their residence or within safe  
 12 deposit boxes. I also know that drug dealers often convert cash proceeds into valuable items  
 13 such as precious metals and gems such as gold, silver, jewelry, *etc.* I also know from  
 14 training and experience that drug dealers often keep records of drug sales and transactions.  
 15 These records are kept so that the drug dealers can keep track of the money owed to them  
 16 for the amount of drugs being sold.

### 17 III. WITTERS's Gemini Account

18 70. According to its website, [www.gemini.com](http://www.gemini.com), Gemini Trust Company is a  
 19 digital asset exchange that allows users to buy, sell, and store digital assets such as  
 20 bitcoins.

21 71. According to records obtained from Gemini, WITTERS opened an account  
 22 (i.e., WITTERS's Gemini Account) in August 2017. WITTERS's Gemini Account is  
 23 linked to WITTERS's Checking Account.

24 72. From approximately October 2017 through October 2018, more than  
 25 approximately 600 BTC were deposited into WITTERS's Gemini Account. These  
 26 deposits included an initial set of deposits made from October 3, 2017, through October  
 27 8, 2017, cumulatively amounting to approximately 121.22269495 BTC (worth  
 28 approximately \$530,808.52 U.S. dollars as of early October 2017). Records indicate that

1 hundreds of purchases and sales of cryptocurrencies (primarily bitcoins) were made via  
2 the account, and that the account's U.S. dollar balance varied from as little as \$0.01 to  
3 \$1,501,937.26. As detailed in a table above, between November 30, 2017, and January  
4 17, 2018, a total of approximately \$800,560.96 was withdrawn from WITTERS's Gemini  
5 Account and transferred to WITTERS's Checking Account.

6 73. As of October 24, 2018, WITTERS's Gemini Account held balances of  
7 approximately \$155,928.01 U.S. dollars and 0.29215414 BTC.

8 74. During my review of WITTERS's Gemini Account, I located several  
9 messages exchanged between WITTERS and Gemini. The messages pertained to the  
10 source of WITTERS's bitcoins. For example, I observed the following message sent by  
11 WITTERS on January 12, 2018:

12 "The coins i purchased at a minute fraction of what they are now and over  
13 the yrs have been converted so many times and sent to exchanges and back  
14 and cross chains there is absolutely no possible way to show it. If i had  
15 deposited 200 bitcoins 2 years ago you wouldn't have even noticed right? I  
16 can't image that I'm alone in suddenly having a large account balance."

17  
18 "I have found proof that I was buying bitcoins on coinbase in 2015, Would  
19 a download of my transactions showing deposits into coinbase in 2015  
20 suffice to show I have been active in buying and trading bitcoins? I can  
21 upload the excel file if you would like. This shows that I was making  
22 deposits into coinbase in December 2015."

23 75. Based on my training and experience, I submit that this information  
24 demonstrates that WITTERS's Gemini account and the bitcoins deposited into that  
25 account (as well as derivative U.S. dollars and cryptocurrencies held in the account) were  
26 the proceeds of, and/or derived from, dark web narcotics sales.

27 76. Based on my training and experience, and as further detailed above, I  
28 believe that Gemini, if served with a warrant to seize cryptocurrencies held in a Gemini

1 user's wallet, is capable of assisting law enforcement with the execution of that warrant  
 2 by, among other things, facilitating the transfer of said cryptocurrencies into a law  
 3 enforcement-controlled wallet. I therefore request that the Court authorize law  
 4 enforcement to execute the requested warrants pertaining to WITTERS's Gemini wallets  
 5 by serving the warrant directly upon Gemini itself.

#### 6 **IV. WITTERS's Robinhood Account**

7 77. Robinhood Markets, Inc. ("Robinhood") is a financial services company  
 8 that allows users to invest in publicly traded companies, exchange-traded funds, and  
 9 cryptocurrencies.

10 78. According to records obtained from Robinhood, from June 2018 through at  
 11 least October 2018, a cumulative total of approximately \$170,000 in funds were  
 12 transferred from WITTERS's Savings Account to a Robinhood account (i.e.,  
 13 WITTERS's Robinhood Account). For example, the following funds were transferred  
 14 from WITTERS's Savings Account to WITTERS's Robinhood Account on or about the  
 15 dates listed below:

Date	Amount
6/13/18	\$20,000
8/22/18	\$50,000
9/5/18	\$50,000
9/24/18	\$50,000
<b>Total =</b>	<b>\$170,000</b>

23 79. As of October 31, 2018, WITTERS's Robinhood Account had a U.S. dollar  
 24 balance of approximately \$167,293.25.

#### 25 **V. WITTERS's Bittrex Account**

26 80. According to its website, [www.bittrex.com](http://www.bittrex.com), Bittrex is a blockchain  
 27 platform that provides users with digital wallets and the ability to execute trades.  
 28



81. According to records obtained from Bittrex, WITTERS opened an account (i.e., WITTERS's Bittrex Account) in July 2016. WITTERS's Bittrex Account is largely funded by deposits of bitcoins. Account records indicate that, from around August 2017 to October 2018, approximately 155 sell orders were executed in which bitcoins were exchanged for units of Tether (another form of cryptocurrency). As of November 8, 2018, WITTERS's Bittrex Account had a balance of 25,936 units of Tether (which are worth approximately \$25,798.74 U.S. dollars at prevailing market rates).

82. Based on my training and experience, and on information described herein, I submit that the bitcoins deposited into WITTERS's Bittrex Account—as well as any derivative assets (including bitcoins or other cryptocurrencies)—are the proceeds of, and/or derived from, dark web narcotics sales.

83. Based on my training and experience, and as further detailed above, I believe that Bittrex, if served with a warrant to seize cryptocurrencies held in a Bittrex user's wallet, is capable of assisting law enforcement with the execution of that warrant by, among other things, facilitating the transfer of said cryptocurrencies into a law enforcement-controlled wallet. I therefore request that the Court authorize law enforcement to execute the requested warrants pertaining to WITTERS's Bittrex wallets by serving the warrant directly upon Bittrex itself.

#### **H. WITTERS's Criminal History and Income**

84. WITTERS's criminal history includes a felony conviction for Possession of a Controlled Substance.


85. After reviewing the transactional histories of WITTERS's Checking, WITTERS's Savings Account, and WITTERS's GBC Savings Account, I was unable to identify any recurring deposits that would suggest that WITTERS was earning a salary, dividends, or other form of recurring legitimate income during the time period of December 2015–October 2018. The only exception appeared to be deposits from the U.S. Government pertaining to Supplemental Security Income (“SSI”) benefits into

1 WITTERS's Checking Account, which from January 2018 to October 2018 cumulatively  
2 amounted to approximately \$29,380.

3 86. I have obtained records from the Washington State Employment Security  
4 Department, after requesting information related to WITTERS. According to records  
5 provided by the Employment Security Department, WITTERS reported a total of  
6 approximately \$5,486 in income during the time period of 2012 through June 2018.

7  
8 **CONCLUSION**

9 87. Based upon the evidence gathered in this investigation and set out above, I  
10 submit that there is probable cause to believe that the SUBJECT ASSETS constitute  
11 property constituting, or derived from, proceeds obtained, directly or indirectly, as the  
12 result of violations of 21 U.S.C. §§ 841(a)(1), (b)(1)(A), and 846 and therefore that the  
13 SUBJECT ASSETS are subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(b),  
14 and 21 U.S.C. §§ 853(a), 853(f), and 881(a)(6).

15   
16 MICHAEL FISCHLIN  
17 Inspector, USPIS  
18

19  
20 SUBSCRIBED AND SWORN before me on this 7<sup>th</sup> day of December, 2018.

21   
22 PAULA L. McCANDLIS  
23 United States Magistrate Judge  
24  
25  
26  
27  
28

**ATTACHMENT A-1**

**Place To Be Searched**

The place to be searched is 5834 NE 75th Street, apt B208, Seattle, WA 98115.

**ATTACHMENT A-2**

**Place To Be Searched**

The property to be searched is an Android phone, model 1+, phone number 206-316-6268, believed to belong to MATTHEW WITTERS.

**Attachment B-1**

This warrant authorizes the government to search for the following items that are evidence and/or fruits of possession of controlled substances with intent to distribute and/or distribution of controlled substances:

1. Any controlled substances, in particular fentanyl
2. Drug Paraphernalia: Items to be used to store and distribute controlled substances, such as plastic bags, cutting agents, scales, measuring and packaging equipment and similar items.
3. Drug Transaction Records: Documents such as ledgers, receipts, notes, books and similar items relating to the acquisition, and distribution of controlled substances, however stored, including in digital devices.
4. Customer Supplier Information: Items identifying drug customers and drug suppliers, such as address and/or telephone books, correspondence, diaries, calendars, notes with phone numbers and names, "pay/owe sheets" with drug amounts and prices, papers reflecting names, addresses, and/or telephone numbers of co-conspirators.
5. Documents reflecting the source, receipt, transfer, ownership and disposition of the United States Currency or other monetary instruments, of real estate and personal property, such as vehicle registration, insurance documents, account bank statements, registers, deposit tickets, concealed checks, loan paperwork, wire transfer receipts, debit and credit tickets, and correspondence.
6. All bank and financial records, including bank statements, wire transfers slips/orders, money order receipts, ATM receipts, cashier checks, cashier check receipts, and safe deposit records for the years 2014 through the present.
7. Rental Agreements, correspondence, keys and entry records for the safe deposit boxes and storage units.
8. Correspondence, papers, records, and any other items showing employment or lack thereof.
9. Records of domestic of domestic and foreign travel such as itineraries, passports, tickets, lodging receipts, and payment records.

10. Records an item identifying smart phones, telephones and pagers used by conspirators including telephone toll bills, pager bills, subscriber agreements, cellular telephones/smart phones and pagers.
11. All firearms and ammunition.
12. Items tending to establish the identity of persons in control of the premises or vehicle being searched.
13. For the Tower, ASUS model, v12xT,
  - a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;
  - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;
  - f. evidence of the times the digital device or other electronic storage media was used;
  - g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;
  - h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

- i. contextual information necessary to understand the evidence described in this attachment.
- j. all documents reflecting cryptocurrencies, including web history, and documents showing the location, source, and timing of acquisition, of any cryptocurrencies

THE SEIZURE OF THE COMPUTER DESCRIBED ABOVE IS AUTHORIZED FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATION OF ITS CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES



**ATTACHMENT B-2**

**Items to be Seized**

This warrant authorizes the government to search for the following items that are evidence and/or fruits of possession of controlled substances with intent to distribute and/or distribution of controlled substances:

- a. Assigned number and identifying telephone serial number (ESN, MIN, IMSI, or IMEI);
- b. Stored list of recent received, sent, and missed calls;
- c. Stored contact information;
- d. Stored photographs of narcotics, currency, firearms or other weapons, evidence of suspected criminal activity, and/or the user of the phone or suspected co-conspirators, including any embedded GPS data associated with those photographs;
- e. Stored text messages.
- f. digital currency applications and wallets, to include information regarding current balance and transaction history, *i.e.*, date, time, amount, and address of the sender/recipient of a digital currency transaction maintained in such wallets;